REMARKS

Claims 1-11 are pending. Claims 1, 7, and 10 have been amended. Claim 11 has been added. Applicants respectfully submit that no new matter has been introduced. Reexamination and reconsideration of this application are respectfully requested.

In the March 22, 2005 Final Office Action, the claims 1, 2, 6, and 10 were rejected under 35 U.S.C. §103(a) as being obvious over U.S. Patent No. 6,453,416 to Epstein ("Epstein") in view of U.S. Patent No. 5,910,989 to Naccache ("Naccache"). Claims 3-5 and 7-9 are rejected under 35 U.S.C. §103(a) as being obvious over Epstein and Naccache in view of U.S. Patent No. 6,654,754 to Knauft et al. ("Knauft") and the publication "HTTP Authentication: Basic and Digest Access Authentication" by Franks et al. ("Franks"). These rejections are respectfully traversed.

Claims 1, 2, 6, and 10

Claims 1, 2, 6, and 10 under 35 U.S.C. §103(a) as being obvious over Epstein in view of Naccache. The Office Action asserted that Epstein discloses a method for obtaining a digital signature involving (a) transmitting a merchant request from a web browser to a merchant server; (b) responding to the merchant request with a specific data string and a request for a digital signature to be appended to the data string; (c) receiving the request for the digital signature; (d) notifying the web browser of the request for the digital signature; (e) obtaining the digital signature from the wireless device; (f) appending the digital signature to the specific data string; (g) notifying the web browser the digital signature has been obtained; and (h) transmitting the data with the appended digital signature to a requesting party. The Office Action also stated that Epstein does not disclose establishing a protected short range wireless line between a computer and the wireless device an transmitting the digital signature from the wireless device to the computer via the short range wireless link. However, the Office Action further stated that

Naccache discloses such wireless link and that it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Epstein and Naccache in the direction of claims 1, 2, 6, and 10.

Claim 1, as amended, recites (with emphasis added):

> 1. A method for obtaining a digital signature comprising the steps of:
> transmitting a merchant request from a web browser to a merchant server;
> **responding to the merchant request with a specific data string having a header, wherein the header includes a request for a digital signature to be appended to the data string;**
> receiving the request for the digital signature;
> notifying the web browser of the request for the digital signature;
> obtaining the digital signature from a wireless device;
> appending the digital signature to the specific data string;
> notifying the web browser the digital signature has been obtained;
> transmitting the data with the appended digital signature to a requesting party;
> establishing a protected short range wireless link between a computer and the wireless device; and
> transmitting, via the short range wireless link, the digital signature from the wireless device to the computer.

Epstein describes providing a secure proxy signing device to form digital signatures which are supplied over an insecure network. Epstein further describes forming a digital signature of a document using a private key stored within the signing device and data items supplied to the signing device from which a document hash is derived and authenticated within the signing device. Epstein still further describes encrypting the document has with the private key to form the digital signature only if the document hash has been authenticated. Naccache describes a method for generating digital signatures for electronic messages, and is directed to enabling smart cards with reduced calculation and storage resources to produce digital signatures with a high degree of security in spite of their reduced resources. Naccache further describes sending a generated digital signature to a verifier device or terminal in which a smart card has been inserted.

However, neither Epstein nor Naccache, alone or in combination, disclose *responding to the merchant request with a specific data string having a header, where the*

header includes a request for a digital signature to be appended to the data string. The Office Action stated that Epstein discloses such responding with a specific data string, referring to FIG. 2 (ref. 46) and Col. 5, lines 4-9 and col. 6, lines 60-63. Applicants respectfully disagree with the Office Action. Specifically, Epstein does not disclose responding with a *specific data string*; instead, Epstein discloses that a "blank document D_0 (which may be integrated in [a Java] applet)" is transmitted. However, this *blank document* does not contain a specific data string. Instead, as its description implies, it is simply a blank document that lacks a *specific data string*.

Moreover, there is no disclosure that the blank document disclosed in Epstein has a *header* that *includes a request for a digital signature to be appended to the data string*. Instead, Epstein merely discloses that the blank document sent to the user is filled out and approved by the user and then sent to a server. Naccache likewise fails to disclose use of the claims "specific data string" or "header." Accordingly, Applicants respectfully submit that claim 1 distinguishes over Epstein, alone or in combination with Naccache. Claims 2 and 6 depend from claim 1 and therefore also distinguish over Epstein, alone or in combination with Naccache, for at least the same reasons as those discussed above with respect to claim 1. Claim 10 contains distinguishing "specific data string" and "header" limitations similar to those of claim 1 and therefore also distinguishes over Epstein, alone or in combination with Naccache.

Therefore, Applicants respectfully that the rejection of claims 1, 2, 6, and 10 under 35 U.S.C. §103(a) should be withdrawn.

Claims 3-5 and 7-9

Claims 3-5 and 7-9 are rejected under 35 U.S.C. §103(a) as being obvious over Epstein and Naccache in view of Knauft and Franks. The Office Action asserted that the combination of Epstein and Naccache fails to disclose the step of recognizing a command with the request for a digital signature. However, the Office Action stated that Knauft disclose a

system of dynamically generating an electronic document and providing access to a resource to a user, and that Franks discloses use of a WWW-Authenticate header containing a command requesting authentication from the user as well as data to be digitally signed and a URL for the response. The Office Action further stated that it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Epstein and Naccache in view of Knauft and Franks in the direction of claims 3-5 and 7-9.

Claims 3-5 depend from claim 1 and therefore distinguish over Epstein and Naccache for at least the reasons discussed above with respect to claim 1. Claim 7 contains distinguishing "specific data string" and "header" limitations similar to those in claim 1. Specifically, claim 1 recites (with emphasis added):

> "7. A method for obtaining a digital signature in a transaction between a computer of a customer and a merchant, comprising the steps of:
> *receiving a request for a digital signature to be appended to a specific data string from the merchant during an electronic transaction;*
> *recognizing a command for the digital signature and the data string to be digitally signed within the request, the command being contained within a header of the data string;*"

Therefore, claim 7, and claims 8-9 depending therefrom, distinguish over Epstein and Naccache for reasons similar to those discussed above with respect to claim 1.

Knauft and Franks do not make up for the deficiencies of the combination of Epstein and Naccache. Knauft is directed to the generation of index information for a data object. Franks discloses a method for HTTP authentication, but is not directed toward the obtaining of digital signatures in a transaction. Instead, it discloses a method of ensuring that a user name and password are sent to a server when the user desires to access an object at the server. [*See, e.g.*, para. 3.2.1]

Accordingly, the combination of Epstein, Naccache, Knauft, and Franks does note disclose, teach, or suggest at least the "specific data string" and "header" limitations of claims 3-

5 and 7-9. Therefore, Applicants respectfully that the rejection of claims 3-5 and 7-9 under 35 U.S.C. §103(a) should be withdrawn.

Claim 11

New claim 11 recites (with emphasis added): "[t]he method of Claim 1, *wherein in response to the request for the digital signature being received from the merchant server, the obtaining of the digital signature is performed without additional interaction from the merchant server.*" None of the cited references disclose that the obtaining of the digital signature is performed without additional interaction from the merchant server disclose in response to the request for the digital signature being received from the merchant server. Epstein, *e.g.*, discloses that user equipment (*e.g.*, a computer) having the browser on which the java applet is being executed, and the browser cannot directly request a digital signature from a smart card reader section of the computer. Instead, it has to sent a command to a server, which routes the command back to the smart card reader section of the computer. Accordingly, additional interaction with the merchant server is required after the request for the digital signature is initially received. Nacchace, Knauft, and Franks also fail to disclose this limitation.

Accordingly, Applicants respectfully submit that new claim 11 distinguishes over a combination of Epstein, Nacchace, Knauft, and Franks.

Applicants believe that the foregoing amendments place the application in condition for allowance, and a favorable action is respectfully requested. If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is requested to call the undersigned attorney at the Chicago telephone number (312) 425-3900 to discuss the steps necessary for placing the application in condition for allowance should the Examiner believe that such a telephone conference would advance prosecution of the application.

Dated: June 22, 2005

Respectfully submitted,

By James M. Wakely

James M. Wakely
Registration No.: 48,597
JENKENS & GILCHRIST, A PROFESSIONAL CORPORATION
225 West Washington Street, Suite 2600
Chicago, IL 60606
(312) 425-8545
Attorney For Applicants